Evaluation Warning: The document was created with Spire.Doc for Python.

**掌心长兴（版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 掌心长兴 |
| 版本 |  |
| 包名 | com.hanweb.cx.activity |
| 域名线索 | 18条 |
| URL线索 | 6条 |
| APP图标 |  |
| 分析日期 | 2025年5月9日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | com.hanweb.cx.activity.apk |
| 文件大小 | 53.37MB |
| MD5值 | e1877e592085acc85a9f3302d6e32fb7 |
| SHA1值 | 4fc0eec909c06be4b271ee9c7e28e90c07d0a7d2 |
| SHA256值 | bc6a22254451526e3ab04fb4385de1911cfa10f31cfebd54c0324911275c3267 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 掌心长兴 |
| 包名 | com.hanweb.cx.activity |
| 主活动Activity |  |
| 安卓版本名称 |  |
| 安卓版本 |  |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.asia | IP: 49.4.35.251 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| unpkg.com | IP: 104.17.247.203 所属国家: United States of America 地区: California 城市: San Francisco  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.com | IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin  |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |
| www.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| data-drcn.push.dbankcloud.com | IP: 49.4.40.58 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| metrics1-drcn.dt.dbankcloud.cn | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.cn | IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| render.alipay.com | IP: 116.136.135.168 所属国家: China 地区: Nei Mongol 城市: Ordos  |
| metrics2.data.hicloud.com | IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://render.alipay.com/p/yuyan/180020010001208736/aliyunFacewelcome.html  | 摸瓜V1引擎  |
| https://metrics1-drcn.dt.dbankcloud.cn:443  | 摸瓜V2引擎  |
| https://metrics-dra.dt.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics2.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.dt.dbankcloud.ru:6447  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| https://developer.mozilla.org/en-US/docs/Web/API/Document/execCommand  | 摸瓜V2引擎  |
| https://data-drcn.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dra.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dre.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-drru.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |
| https://grs.platform.dbankcloud.ru  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |
| https://unpkg.com/pdfjs-dist@2.3.200/cmaps/';  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 14517244555  | 摸瓜V1引擎  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: CN=yuhui 签名算法: rsassa\_pkcs1v15 有效期自: 2011-09-23 10:09:55+00:00 有效期至: 2111-08-30 10:09:55+00:00 发行人: CN=yuhui 序列号: 0x4e7c5af3 哈希算法: sha1 md5值: ec18b4135488732564581a0c2dacc1de sha1值: a1b286a7eff84c7dc7226d8413f49272513356e7 sha256值: 246c0680e2f2db1a4c9455b5d50876e5a5a894155fd43fdf8c756922fc6d432f sha512值: b6f1c06510343de7d53a155e4bc2e3e9cd3ad1e4e9a8d527f530bcf1de1e3b8131cbceba8ac5ce55d34507d1a7f9521f59e7dc179e4b5e62376338cb3872310e 公钥算法: rsa 密钥长度: 1024 指纹: 681af32153a4f78c59366ec030429b05be547755c412d9a7325f781ddeb512e6**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "login\_phone\_auth\_code\_get" : "发送验证码"  |
| "order\_detail\_connect\_user" : "联系人"  |
| "password" : "请输入密码"  |
| "security\_public\_key" : "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8hzUojzHX8jDL+97pqr7CaLiKSsZ0aOES7FUcX7vh9PoEDbCKNCTakRXdS5EiurPk3QpvsAGbfyIs7JWKm4py9KcIdJsZRh9onknVeAVlU++jnrGFGEYfQb8iKzClN059gYeeJBs9mwi7RGU9tj0KHUG659v5sMBxv7zNse3fJQIDAQAB"  |
| "set\_user\_name" : "姓名"  |
| "user\_name" : "请输入手机号"  |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 此APP的危险动作**

| 向手机申请的权限 | 是否危险 | 类型  | 详细情况 |
| --- | --- | --- | --- |
|  | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**